LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

(ISSN: 2583-7753)

Volume 2 | Issue 1

2024

© 2024 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com
Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal LegalResearch has decided to publish this submission as part of the publication.

In case of **any suggestions or complaints**, kindly contact info.lijdlr@gmail.com

To submit your Manuscript for Publication in the **LawFoyer International Journal of DoctrinalLegal Research,** To submit your Manuscript Click here

DEEPFAKE TECHNOLOGY AND LEGAL ISSUES

Deeksha Kumari[1]

I. ABSTRACT

The advent of social media has united the entire world into one enormous country. We have access to news from all around the world because of the internet. A few years ago, a unique approach that made it simple to edit photos and films emerged, providing incredible technology that entertained people. This method, which was first employed by people to amuse or play practical jokes on others, swiftly evolved into one of the riskiest things available on the internet right now. The deep-learning technology used in deep fakes has turned the internet into a trap. This study paper aims to comprehend the effects that deep fakes have on society, talk about the laws that prohibit these kinds of actions, and raise awareness about the sharing of these kinds of contents. As English clergyman Thomas Fuller said, "Seeing is believing," yet when it comes to deep fakes, one can no longer trust what they are seeing. Deep fakes are dangerous for both society and individual privacy because of this. They are inexpensive to produce, but when used improperly, they have the power to sway public opinion, control large crowds to incite discontent in the community, and lead to invasions of privacy, to mention a couple of their problems.

The existing legal framework in India does not adequately address cyber offenses resulting from the usage of deep fakes. It is challenging to adequately govern the use of artificial intelligence, machine learning, and deep fakes due to the absence of specific regulations relating these technologies in the IT Act, 2000. It could be essential to amend the IT Act, 2000 to include sections that expressly address the use of deepfake and the penalties for their misuse in order to better regulate offenses caused by them. This would entail tougher legal safeguards for people whose likenesses or photos are exploited

[1] LLM STUDENT (IMS UNISON UNIVERSITY DEHRADUN)

© 2024. LawFoyer International Journal of Doctrinal Legal Research (ISSN: 2583-7753)

without their permission, as well as harsher punishments for those who produce or disseminate deep fakes with malevolent intent.

II. KEYWORDS

Deep fakes, Artificial Intelligence, Machine Learning Algorithm, Indian Law, Pornography, Terrorism, Indian Penal Code, Information Technology Act, Defamation, Block chain Technology

III. INTRODUCTION

Deep fakes are dangerous to both society and individual privacy. They are inexpensive to produce, but when used improperly, they have the power to sway public opinion, control large crowds to incite discontent in the community, and lead to invasions of privacy, to mention a couple of their problems. An artificial intelligence technique called "deepfake AI" was used to produce realistic-looking photos, audio, and video hoaxes. [2] A word, which is a combination of deep and fake learning, refers to both the technique and the phony information that results from it. Deep fakes usually include the replacement of one individual in pre-existing source material with another. They also create entirely original videos, where actual people are depicted saying or acting in ways they have never done. In 2017, public awareness was created when an anonymous Reddit user with the username "deepfake" uploaded a series of videos. These were not just videos; however, they were deepfake, in which the faces of famous people, mostly female actors, were artificially superimposed on pornographic content. [3] The deep fake technology was then applied to the user's moniker, the deep faker. Following this, comparable pornographic deepfake movies went viral, causing a number of celebrities and even members of the general public to fall victim to content. Furthermore, some deepfake movies featuring officials, such as Obama and Trump, have surfaced, gravely jeopardizing diplomatic security and the country's reputation.

[2] https://seotoolboxs.online/deepfake-ai-a-powerful-tool/11/2023
[3] Marr, B. The Best (And Scariest) Examples Of … July 22, 2019

IV. TECHNOLIGY FOUNDATIONS

Two methods are used to create a deepfake image: deep learning and generative adversarial networks. Artificial neural networks, a subsection of deep learning, are used to process and analyze massive volumes of data using algorithms modeled after the structure and operation of the brain. Numerous fields, including computer vision, robotics, speech recognition, and natural language processing, have benefited from deep learning. A type of deep learning architecture known as generative adversarial networks (GANs) trains on a dataset to produce new synthetic data that is similar to the original data using two neural networks, a discriminator, and a generator. [4]

A. Auto encoder

The encoder and decoder are two components of the auto encoder artificial neural network design. [5] To compress and encode facial images, the encoder extracts the features from the image and converts them into vector values in the latent space. Meanwhile, the decoder reconstructs the original face using the features extracted by the encoder, bringing the data as close as possible to the input data of the encoder.

To allow for source and target picture face exchange, two pairs of encoder-decoder are needed. The parameters of the two sets of input images were shared by the two encoders, which then used distinct decoders to reconstruct the images during decoding. [6]

[4] Jia Wen Seow, et al., "A Comprehensive Overview of Deepfake: Generation, Detection, Datasets and Opportunities", 513 Science Direct 351-371 (2022) accessed on 6-2-2023.
[5] [16] Ramadhani K N, Munir R. A Comparative Study of Deepfake Video Detection Method [C]//2020 3rd International Conference on Information and Communications Technology (ICOIACT). IEEE, 2020: 394-399.
[6] Yuzhi Zhang, Ruifang Wang, Liang Zhu, et al. The Review of Generation and Detection Techniques for Deepfakes [J]. Journal of Information Security Research, 2022,8(03):258-269.

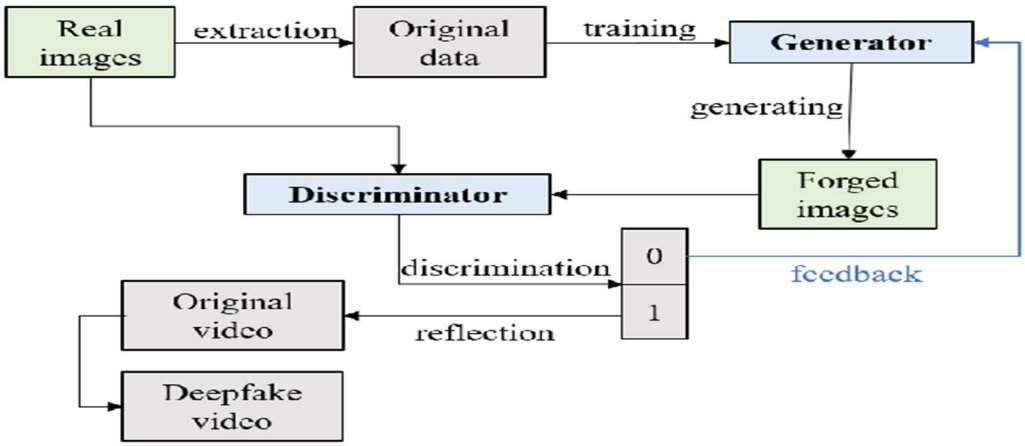
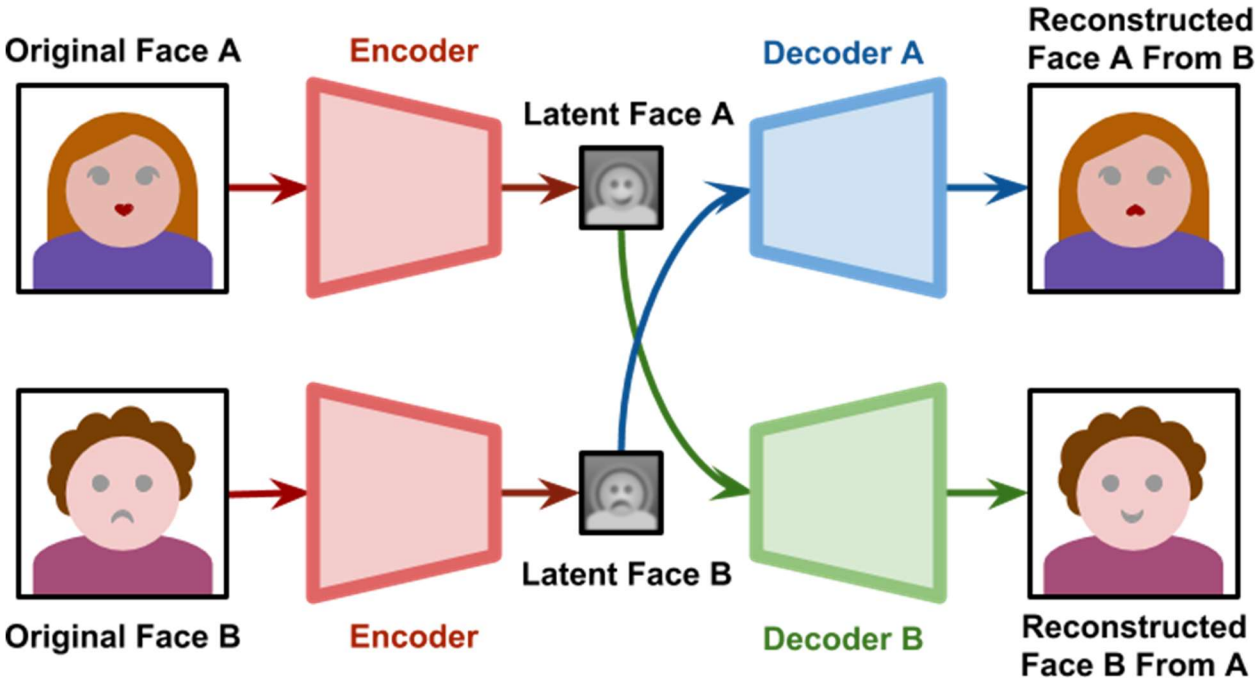


Figure 1. Deepfake generation based on Generative Adversarial Network[7]

However, the auto-encoder network needs to deliberately approximate the probability distribution of the real sample data to improve the fidelity of the deepfake, resulting in insufficient network generalization performance and limited generated fidelity. [8]



[7] Min Liu, Xijin Zhang. (January 2023).Deepfake Technology and Current Legal Status of It, In book: Proceedings of the 2022 3rd International Conference on Artificial Intelligence and Education (IC-ICAIE 2022) (pp.1308-1314)

[8] https://www.researchgate.net/figure/Deepfake-generation-based-on-Autoencoder-First-the-two-encoders-extract-facial-features_fig1_368495639

Figure2. Deepfake generation based on Auto encoder[9]

B. Generative Adversarial Network

In Generative Adversarial Networks, Ian J. Good fellow et al., introduced the GAN technology as the fundamental paradigm of "deepfake" in October 2014.In the context of game theory, its core concept originates from a two-person zero-sum. Conventional deep learning In essence, technology is a single-level process, but GAN presents a "adversarial" method that is dependent on the frequent development and identification of internal computerized data. GAN is executed in both directions by learning using two sets of deep convolutional neural networks comprising the discriminator and generator in a dynamic manner[10]. Using this training data, deep fakes are produced that can be used in a variety of ways for both images and videos.

(a) Face Swapping: substituting one person's face for that in the video. [11]

(b) Attribute Editing: altering the video subject's appearance, such as hair color or style.

(c) Face Re-Enactment: projecting the subject's facial expressions from one person's face onto the subject in the target video; as well as

(d) Synthetic material: although real material is used to train people's appearances, the final image is completely artificial.

V. OFFENCES AND LEGAL ISSUES

A. Women-targeting deep fakes: Non-consensual pornography makes up about 96% of deep fakes on the internet. This was also the first time deepfakes were used maliciously. Deep fakes are a simple technique for emotionally attacking and damaging women's reputations. Deep fakes are used to sexually and mentally

[9] Https://Www.Alanzucconi.Com/2018/03/14/Understanding-The-Technology-Behind-Deepfakes/
[10] SCC Online database Report on Deepfack Technology, (17 march 2023)
[11] https://www.researchgate.net/figure/Deepfake-generation-based-on-Autoencoder-First-the-two-encoders-extract-facial-features_fig1_368495639

deceive women. Deep fakes threaten and treat women as objects of desire. Most cases end abruptly in the middle of the inquiry because it is difficult to find the individuals responsible. Pornographic content can be shared through groups and pages on Facebook, Instagram, WhatsApp, or other platforms. The Women-Targeting deepfakes may be subject to Section 292 (Obscene acts or words in public) if it contains sexually provocative or offensive content, and Section 354A (Stalking) can be applied if a woman is being stalked or intimidated by means of a deep fake under Indian penal code 1860. The application of Section 67 of the Information Technology Act 2000 (Publication or transmission of obscene material in electronic form) is applicable in cases when the deepfake contains explicit sexual content. Section 67A (Publication of or circulation of offensive material) for the prosecution of deepfakes that are insulting or disparaging of women.

B. **Deepfakes is meant to defame brands, goods, services, and people**: Using the simple technology Deepfake, one can anonymously disparage a brand, business, good, or person. Because legal action can only be taken against a real person, this is a complex situation. It is typically impossible to find a guilty party hiding behind a phony profile. With the use of artificial technology, people are depicted as engaging in antisocial behavior and saying offensive things to disparage others. Even if they are able to use an alibi to clear the offender, most of the time it is too late, and the offender's reputation has already been damaged. Deepfakes are covered in section 499 of the Indian Penal Code, which prohibits defamation through any medium. It punishes anyone who creates or disseminates any false statement, imputation of behavior, inclination, temperament, or belief that harms someone's standing in society or damages their reputation. The Delhi High Court in the case of **Anil Kapoor v. Simply Life India and the Ors**.[12]protected actor personas and personal characteristics from being misused, particularly when using AI techniques to create deepfakes. The actor's name, likeness, and image

[12] 2023 LiveLaw (Del) 857

were effectively prohibited from being used for financial benefit or commercial purposes by sixteen (16) entities by the court's ex-parte injunction, which also prohibited them from using technical tools such as artificial intelligence.

C. **Intellectual Property Rights (IPR):** AI-generated content and deep fakes frequently alter pre-existing copyrighted items. This calls into doubt the infringement of the rights of copyright holders. The distinction between artificial intelligence (AI) and human creativity may become hazier in court cases involving ownership and control of AI-generated creative works. A significant ruling in **India's Yahoo! Inc. v. Akash Arora and Anr**[13] case highlighted the significance of safeguarding intellectual property rights in the digital arena, especially with regard to trademarks and domain names. According to Section 17 of the Copyright Act of 1957, the original ownership rights to a creation belong to the creator or the writer. The photographer is the author of the photograph, and the video producer is the author of the video format. Furthermore, copyright holders and other individuals who use any part of the work, including photos, are granted exclusivity in licensing under section 14 of the Act, even if they violate the section. It is also important to highlight that deepfakes, especially those that are frequently employed with malicious intent, will not be protected by the defense of fair dealing under Section 52, which encompasses a wide range of actions that do not violate copyright. Sections 63 and 55 of the Act give rise to both criminal and civil actions for infringement, respectively. Liability also results from the IT Act and IPC implementations. At the **Gramophone Company**, the Delhi High Court ruled that artificial intelligence (AI)-generated music created by a computer program lacks human originality and is not entitled to copyright protection. [14]

D. **Right To Privacy and Deepfakes:** It is possible to use deep fakes to produce phony audio or video clips that damage someone's reputation. Deepfake defamation

[13] 1999IIAD(DELHI)229, 78(1999)DLT285
[14] 2010 SCC Online Del 4743 The Gramophone Company of India v. Super Casstte Industries Ltd.

victims may file a lawsuit to recover from the damage to their reputation. Invasion of private life through the use of modified content may also constitute a violation of privacy rights. The Supreme Court of India recognized the right to privacy as a fundamental right in compliance with Indian law in the historic decision of **Justice K.S. Puttaswamy, (d) v. Union of India**[15]. The decision places strong emphasis on protecting personal data from AI-based systems and human rights. Section 66E of the Information Technology Act, 2000 (IT Act) pertains to deepfake offenses that entail the acquisition, dissemination, or publication of an individual's photographs in mass media, thereby infringing their privacy. A fine of ₹2 lakh or up to three years in prison are the possible penalties for this kind of offense. A new law pertaining to the handling of personal data in India is the Digital Personal Data Protection Act of 2023. Almost six years after the Supreme Court upheld the basic right to privacy under Article 21, it was ultimately adopted. The following organizations are eligible to apply for the Digital Personal Data Protection Act 2023:

- The organization handles digital personal data that can be used to identify the data principle, which is the rightful owner of the acquired information.
- The organization gathers the data processed in a digital format.
- The organization processes personal data on Indian soil, or if personal data are processed outside India but in relation to an activity that provides products or services to people in India.

E. Criminal Offenses: Deep fakes can be utilized for fraud and impersonation, which may result in financial losses and cybercrimes. Legal repercussions may exist if explicit deepfake content is created and distributed without permission. Although deepfakes and AI-related crimes are not specifically covered by any law in India, there are provisions under numerous statutes that may provide remedies. For

[15] https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case.

cybercrimes related to deepfakes, Sections 509 (words, gestures, or acts intended to offend a woman's modesty), 153 (a) and (b) (spreading hate on communal lines) 499, which deal with criminal defamation, and of the Indian Penal Code, 1860, (IPC) may also be invoked. Using deepfakes to assume someone else's identity, fabricate personal narratives, or sway public opinion can damage someone's credibility and reputation, while disseminating misleading information. These offenses are punishable under section 66 (computer-related offences) and section 66-C (punishment for identity theft) of the Information Technology Act of 2000.Recently, a deep fake video of Indian actress Rashmika Mandanna went viral in November 2023. She described the event as "extremely scary." [16] The singer Taylor Swift is the most well-known victim of the epidemic of pornographic deepfake photos created by artificial intelligence, which sexualizes people without their consent. This issue is difficult for digital platforms and anti-abuse agencies to address. On the website of social media X, false pictures of Swift that were abusive and sexually graphic started to go viral. [17]

F. Misinformation and Election Manipulation: Deep fakes and other AI-generated content may be used to propagate false information during elections. To stop the abuse of these technologies and control political discourse, legal action is required. Two edited video clips featuring superstar Amitabh Bachchan from "Kaun Banega Crorepati" in Madhya Pradesh, which is set to hold elections, depict Chief Minister as a liar and positively portray Opposition candidate. Prior to the 2024 elections, the Federal Election Commission (FEC) in the US started an effort this year to potentially limit the use of all AI-generated deepfakes in political commercials. [18] According to Techarc data, the number of smartphone users in India has grown from just over 500 million in 2019 to over 650 million in 2023.This increase poses a severe danger to India's youthful voter base, as does the widespread availability

[16] 1 Feb 2024 India Today
[17] https://toronto.citynews.ca/2024/01/26/deepfake-explicit-images-taylor-swift/
[18] article/fec-artificial-intelligence-deepfakes-election-2024-95399e640bd1e41182f6c631717cc826

of inexpensive, high-speed Internet and sophisticated analytics used by political consultants. [19]

Section 66-F of the Information Technology Act of 2000 deals with cyber terrorism offenses, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022, deal with cases related to Misinformation against Governments. Additionally, Section 121 of the Penal Code, 1860 (waging war against the Government of India), and Section 124-A could be used in these cases. Prior to the state election earlier this month, the Party employed artificial intelligence technology to produce two deepfakes of its leader, morphing him accurately to appear as though he was speaking in two languages: Artificial intelligence (AI) is used by Deepfake to produce morphing films that look authentic and can even speak for other people. [20]

G. **Consumer Protection and Fraud:** By creating realistic scams, deepfakes can draw people into fraudulent operations. Deepfake-related offenses should be added to laws that deal with digital fraud. To encourage people to believe that celebrities and other well-known public figures are profiting greatly from online investment trading platforms, scammers are fabricating deepfake videos and fake news articles.

- **Product or Service Misrepresentation:** Deepfake can be used to fabricate expert or celebrity endorsements for market goods or services. Customers may be misled by this to think that a product is superior to what it is truly.
- **Financial Scams:** By seeming to be real individuals, such as CEOs or corporate reps, deepfake fool's customers to give money or disclose personal information.

[19] https://techarc.net/wp-content/uploads/2023/05/Techarc-Trends-India-Smartphone-Industry-2023
[20] 20 Feb 2020 NDTV News

Through the use of deepfake technology, a finance employee at a multinational corporation was duped to give $25 million to con artists posing as the company's chief financial officer during a video conference call. [21] A resident of Kozhikode, Kerala, lost ₹40,000 when cybercriminals pretended to be former colleagues in a WhatsApp video chat and asked for money to pay for his sister's operation using deepfake AI technology. [22]

H. **Authenticity of evidence:** The authenticity of evidence in court cases may be jeopardized because it is simple to create convincing deepfakes. It may be necessary for courts to use cutting-edge methods to validate digital evidence. Digital evidence is inherently volatile and subject to change, in contrast to physical evidence, which is easily sealed and maintained.[23]To uphold the adversarial concept in criminal processes, defendants must be afforded the chance to contest the admissibility of evidence.

   On the other hand, defendants may not be able to question decisions made using deep fake evidence because of the technical complexity of AI systems without the need for expert aid, which would incur additional expenditures. The inability of AI systems to be transparent makes it more difficult for defendants and their attorneys to challenge the reliability of evidence produced using techniques that programmers find difficult to comprehend. Since the current legal standards are out of date and there is no special mechanism for confirming the authenticity of manipulated evidence in courtrooms, it is vital to assess if the current rules are adequate for identifying deepfakes.[24]

I. **International threats involving deep fake:** Deepfake is becoming a serious danger to world peace and security. They can be used as weapons to stoke international

[21] https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
[22] 18 Jul 2023 live Mint Report
[23] Central Bureau of Investigation. (2020). Cyber Crime Investigation Manual
[24] https://whatnext.law/2024/02/26/ai-through-the-looking-glass-addressing-evidence-authenticity-in-the-deepfake-era

strife and to influence public opinion. Consider a staged film purporting to show a foreign leader saying offensive things. This may lead to diplomatic problems or even military build-up. Deepfake is another way in which elections might be tainted by malevolent actors who disseminate false information to topple governments or harm the standing of rival candidates. Another possible application is economic espionage, in which falsified movies deceive executives into disclosing private information, thereby undermining a country's ability to compete internationally.

Deepfake can even be used as a tool for cyber warfare, causing havoc throughout a country or for upsetting vital infrastructure. Imagine a faked video that ignites civic upheaval or a deepfake news item, generating panic in financial markets. Shortly after Russia began an extensive invasion of neighboring Ukraine on March 2, 2022, a short video message featuring the Ukrainian President briefly surfaced on the news website Ukraine 24. [25] Zelenskyy pleaded with the Ukrainians to give up their weapons and surrender, not to continue fighting. Unexpectedly, the video soon gained popularity on VKontakte, Telegram, and other social media sites where it was discovered and covered by international media. [26]

J. Liability and Accountability: It is difficult to establish who is responsible for harm caused by AI-generated content. Platforms, users, and developers of AI should all have responsibilities addressed by legal frameworks.

- **Deepfake Creator:** The person who creates the deepfake with malicious intent can be held liable for the crime committed using the deepfake. This could involve charges like fraud, defamation, or election interference depending on the specific use. Existing laws like those against forgery (Section 468 Indian Penal Code), impersonation (Section 416 Indian Penal

[25] The Telegraph, "Deepfake video of Volodymyr Zelensky surrending surfaces on social media," YouTube, March 17, 2022

[26] Tom Simonite, "A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be," WIRED, March 17, 2022

Code), and cybercrime can be applied depending on the nature of the deepfake. For instance, creating a deepfake to damage someone's reputation could fall under defamation laws (e.g., Section 499 of the Indian Penal Code).

- **Deepfake Distributor:** The Person who knowingly distributes the deepfake, especially if it is intended to cause harm, can also be held liable. This could include individuals sharing deepfakes on social media or platforms that fail to reduce harmful content after notification. Laws concerning aiding and abetting a crime or spreading misinformation may also be applicable. Additionally, consumer protection acts with provisions on unfair trade practices (e.g., Section 2(a) (ii) of the Consumer Protection Act, 2019 (India)) could be used against platforms that do not address deepfake.
- **Social Media Platforms:** Social media platforms might face increased scrutiny due to inadequate measures to detect and remove deepfakes. Some countries have introduced specific regulations on online platforms. For instance, India's Information Technology Act, 2000 (amended with IT Rules, 2023), outlines the diligence requirements for significant social media intermediaries. Failure to comply can lead to a loss of immunity protection from lawsuits.

VI. EXISTING LEGISLATION OF DEEPFAKE

A. Right to privacy

The Since the Supreme Court of India's 9-judge ruling in **Justice KS Puttaswamy (Retd.) v. Union of India's**[27] right to privacy has been acknowledged as a Fundamental Right. This originates in Article 21. Therefore, it is a fundamental right to use someone else's personal information, such as images and videos, without that person's consent.

[27] AIR 2018 SC (SUPP) 1841

Additionally, under section 66E of the IT Act, someone who willfully and intentionally takes a picture of someone else's private area and publishes it online or transmits it without that person's consent faces up to three years in prison, a fine of up to two lakh rupees, or both.

B. The Information Technology Act, 2000

When someone is the victim of a deepfake crime—that is, when their photos are taken, published, or transmitted in the media, invading their privacy—they are subject to Section 66E of the IT Act of 2000. The maximum penalty for this offense is ₹2 lakh in fines or three years in prison. Section 66D of the IT Act is another relevant section. A clause of the law stipulates that anyone who utilizes computer resources or communication devices maliciously to deceive or impersonate someone may face up to three years in prison and/or a fine of up to ₹1 lakh. The IT Act's provisions in question may be used to bring criminal charges against those responsible for deepfake cybercrimes in India.

C. Indian Copyright Act of 1957

Penalties for some offenses, such as copyright infringement, are outlined in Section 51. It forbids using any property that belongs to someone else and over which that person has the sole right without permission. Provisions of Indian law forbid fraud, including financial and identity theft. If anyone uses videos, images, or the voice of another person to create a deepfake, and that deepfake incorporates copyrighted material, it could be punishable under Section 51 of the Copyright Act.

VII. SUGGESTED LAWS AND PROVISION REQUIRED

A. **Define deepfake:** Like American Malicious Deep Fake Prohibition Act of 2018[28] India needs to define the deepfake technology. The bill broadly defines deep fakes as any media that falsely "appears to authentically depict any speech or conduct of a person," and produced substantially by "technical means."

[28]https://www.congress.gov/bill/115th-congress/senate-bill

B. **Civil and criminal Liability:** Deep fakes give rise to both criminal and civil liabilities and it is necessary for the law and judiciary to differentiate these liabilities as the impact of deepfakes is more serious than we can imagine. The recent case of Gabon when deepfake video led to a military coup and political instability. [29]

C. **Creators' accountability**: Law should have been decided who is responsible for what, and most classes of deepfakes should have been required to carry digital watermarks and prominent textual or audio disclaimers stating the amount of the alterations. Furthermore, the government ought to have established a national security task force to construct detection tools and share them with internet platforms, amended false personation laws to include digital impersonation, and established an in rem litigation procedure to sue creators of deepfakes who cannot be identified.

D. **Evidence Law in case of deepfake:** Deepfake evidence has already shown to be a serious issue and attracted a lot of attention. In a UK case where a mother attempted to use her husband's menacing audio remarks against him during a custody battle for their children, the husband was able to prove that the audio recording was phony, having been made by software that used metadata analysis to imitate his voice. Even though the audio file's falsification was eventually discovered in that instance, the story serves as a warning about the potential for deepfakes to provide false evidence and a sneak peek at what may happen in the future as deepfakes become more prevalent in legal procedures. There is the need of technological advancement in field of evidence law and the experts should hired in these cases. [30]

[29] https://www.washingtonpost.com/politics/2020/02/13/how-sick-president-suspect-video-helped-sparked-an-attempted-coup-gabon/

[30] 31 Jan 2020 The Telegraph

E. **'Defending Person from False Appearances:** US Congress passed DEEPFAKES Accountability Act in June 2019[31] which main purpose is to Defending Each and Every Person from False Appearances by Keeping Exploitation. India also needs a similar type of law because recently we saw that videos of actors and actresses went viral on social media in which they were shown in misappropriate. [32] A video purportedly featuring Rashmika Mandanna went viral last week, but it was eventually discovered to be a deepfake. The video caused immense humiliation to the actresses. [33]

F. **The Challenges Deepfake Pose in Court:** In court proceedings, deepfake pose three unique challenges: (1) establishing the authenticity of digital images or audio evidence; (2) answering the "deepfake defense," which is the claim that legitimate digital images or audio evidence is a deepfake; and (3) addressing jurors' growing mistrust and doubt regarding the veracity of all digital images and audio evidence. The Indian judiciary needs to overcome these challenges as the number of cases and their complexity are increasing day by day.

G. **Specific legislation for deepfake and artificial content:** There isn't a law or legislation that addresses deep fakes in India either explicitly or directly. Prior to the 2020 elections in the United States, the Deep fakes Accountability Act, 2019 was approved, requiring deep fakes to have a watermark for identifying purposes. A bill that made it illegal to fabricate false footage with the intention of influencing an election result was previously passed in Texas. Comparably, California enacted a law that forbids the production and dissemination of deep fakes about any candidate 60 days before an election, primarily to stop the dissemination of false information among voters in advance of the US 2020 elections. While deep fakes

[31] https://www.congress.gov/bill/116th-congress/house-bill/

[32] DEEPFAKES Accountability Act 2019

[33] 20 Jan 2024 Indian Express

are now included by Virginia's enlarged retaliation porn law, which went into force in 2014. [34]

VIII. CONCLUSIONS

The existing legal framework in India does not adequately address cyber offenses resulting from the usage of deep fake. It is challenging to adequately govern the use of artificial intelligence, machine learning, and deep fake due to the absence of specific regulations relating these technologies in the IT Act, 2000. It could be essential to amend the IT Act, 2000 to include sections that expressly address the use of deepfakes and the penalties for their misuse in order to better regulate offenses caused by them. This would entail tougher legal safeguards for people whose likenesses or photos are exploited without their permission, as well as harsher punishments for those who produce or disseminate deepfake with malevolent intent. Additionally, it's crucial to keep in mind that the development and usage of deepfake is an international issue, and that effective international coordination and collaboration will most likely be required to limit their use and put an end to privacy violations. While this is going on, it's imperative that individuals and institutions understand the potential risks associated with deepfake content and proceed with caution when confirming the accuracy of any information they come across online.

In the interim, governments might choose from the following options: The first kind of Strategy is censorship is giving orders to intermediaries and publishers to prevent the public from getting misleading material. The second Strategy is the punitive approach, which imposes accountability on organizations or individuals for disseminating or producing misleading information. Third Strategy is that the Online intermediaries are required to take down content from their website as soon as a user or government agency reports it that they believe is false or misleading. This helps prevent deepfake from spreading, which might be dangerous or used to manipulate public opinion. Section 79(3)

[34] 15 Dec 2023 Bloomberg Law News

(4) of the Act outlines the potential repercussions of non-compliance. If an intermediary fails to remove content that is obviously untrue or deceptive after receiving a valid notification, they risk losing the legal immunity that shields them from lawsuits originating from user-generated content. This might have major legal and financial repercussions for the platforms.